פרויקט בקורס

תקשורת מחשבים

האיש שבאמצע (MITM)

עבור פרופ' יעקב אקסמן

מגישים:

בר דויטש 208241539 bardoitch@gmail.com

אופיר כהן 316322882 ofircohen0711@gmail.com

טל לוי 311460588 talevon1515@gmail.com

פרויקט בקורס

תקשורת מחשבים

מבוא:

Address Resolution Protocol (ARP) – פרוטוקול תקשורת מבוסס Internet Protocol (IP),
המיוחס לשכבת הקשר (Layer).
פרוטוקול זה משמש לאיתור כתובות MAC (physical address) בהתאמה לכתובות הIP.
בעצם מאחורי הקלעים פרוטוקול זה ממיר את כתובת הIP (32bit) לכתובת MAC (48bit).

איך זה נעשה? בשכבת הקשר, כאשר המקור רוצה למצוא את כתובת ה MAC של היעד הוא תחילה יחפש ב ARP Cache הידוע בשמו גם ARP Table, שם ימצאו כל המכשירים שנוצר איתם קשר בפרוטוקול זה.
במידה והוא לא נמצא שם, המקור יוצר בקשת ARP עם כתובת ה IP הרצויה אותה הוא מחפש, במידה ואותו יעד נמצא ב LAN network הוא יגיב בהודעת ARP ובה ימצא כתובת MAC של אותו יעד התואם את כתובת הIP ואז המקור יעדכן את טבלת הARP לפניות עתידיות.

מכיוון שפרוטוקול זה אינו מאובטח ונועד להיות פשוט ויעיל, אין דרך למקור לאמת שאכן אותה כתובת MAC הינה הכתובת האמתית של אותה כתובת IP. באמצעות חולשה זו ניתן להתחזות לכתובות ברשת המקומית וכך המקור יעדכן את טבלת הARP בהתאם.

מתקפת "האיש שבאמצע" הידוע בשמה MITM נעזרת בחולשה זו ו"מרעילה" את טבלת ה ARP, משנה את ערכיה ובכך מתחזה למשתמש אחר המחובר למקור ואפילו למקור עצמו עבור אותם מכשירים המחוברים לרשת המקומית.

מטרת הפרויקט:

להעמיק בפרוטוקול ARP .

לדמות את המתקפת איש שבאמצע (MITM) בעזרת שימוש בפרוטוקול זה, באמצעות שימוש ברשת אלחוטית, לגלות לאיזה מידע נוכל לגשת באמצעות תקיפה זו ולאיזה לא.

להעמיק בנושא האבטחה וכיצד ניתן לעקוף את חולשת פרוטוקול הARP.

מה בוצע:

על מנת לממש את תקיפת "האיש שבאמצע" תחילה היה עלינו לגשת לנתב אלחוטי המספק רשת WIFI ואל רשת זו נחבר את הקורבן שלו נקרא בניסוי שלנו בוב.

כעת נוכל לראות את הנתונים הבאים:

1. בעזרת הפקודה **ipconfig** נוכל לראות את:

```
C:\Users\□□ □□□□□>ipconfig

Windows IP Configuration
```

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2a00:a040:196:e256::100c
   IPv6 Address. . . . . . . . . . . : 2a00:a040:196:e256:10b5:67a4:8032:28ed
   Temporary IPv6 Address. . . . . . : 2a00:a040:196:e256:7d23:f5fb:87ce:83b8
   Link-local IPv6 Address . . . . . : fe80::10b5:67a4:8032:28ed%10
   IPv4 Address. . . . . . . . . . . : 192.168.1.59
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::ae3b:77ff:fe58:fed2%10
                                       192.168.1.1
```

Ipv4 – כתובת של 32 סיביות שמזהה באופן ייחודי ממשק רשת במחשב.

Subnet Mask- מספר הסיביות בכתובת הIp המשמשות לקביעת כתובת הרשת.

Default Gateway – כתובת הIp שאליה התעבורה נשלחת כאשר היא מיועדת אל מחוץ לרשת הנוכחית (הרשת המקומית).

זה יהיה הקורבן בניסוי, ייצג את בוב.

פרויקט בקורס

תקשורת מחשבים

2 . בעזרת **ifconfig** (במערכות הפעלה linux) המקבילה לipconfig (במערכות הפעלה windows)
נוכל לראות את:

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.92  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 2a00:a040:196:e256::100f  prefixlen 128  scopeid 0x0<global>
        inet6 2a00:a040:196:e256:5af1:6659:563e:1a9  prefixlen 64  scopeid
0x0<global>
        inet6 fe80::8c4e:d893:81d7:568d  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b2:e6:69  txqueuelen 1000  (Ethernet)
        RX packets 5045  bytes 1033383 (1009.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 707  bytes 51394 (50.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12  bytes 596 (596.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12  bytes 596 (596.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Eth0 שם המייצג את ממשק החיבור לאינטרנט.

וכמובן את כל פרטיו האחרים.

3. שימוש בכלי שנקרא **nmap-** כלי לסריקת רשת, המאפשר צפייה בכל כתובת Ip המשתמשות ברשת המקומית.
כלי זה מותקן ומותאם עבור מערכת ההפעלה Linux-kali כמו שאר הכלים איתם נעבוד ולכן בחרנו להשתמש במערכת הפעלה זו המותאמת עבור דימוי מתקפה שכזאת.
על מנת להתקין כלי זה יש לרשום את השורה הבאה : sudo apt-get install nmap

```
┌──(root💀 kali)-[~]
└─# sudo nmap -sn 192.168.1.0/24
```

כתובת שמחזירה את כל הכתובת שנמצאות ברשת המקומית.

מספר הסיביות הדלוקות ב- subnet mask

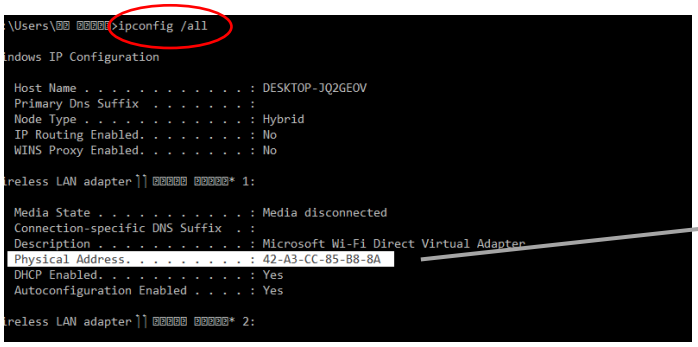
```
root@kali: ~
File  Actions  Edit  View  Help

┌──(root㉿kali)-[~]
└─# sudo nmap -sn 192.168.1.0/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-06 11:00 UTC
Nmap scan report for 192.168.1.1
Host is up (0.054s latency).
MAC Address: AC:3B:77:58:FE:D2 (Sagemcom Broadband SAS)
Nmap scan report for 192.168.1.3
Host is up (0.049s latency).
MAC Address: D8:7D:7F:09:21:8F (Sagemcom Broadband SAS)
Nmap scan report for 192.168.1.4
Host is up (0.054s latency).
MAC Address: D8:7D:7F:09:21:95 (Sagemcom Broadband SAS)
Nmap scan report for 192.168.1.5
Host is up (0.054s latency).
MAC Address: 76:CB:0E:A6:5A:18 (Unknown)
Nmap scan report for 192.168.1.10
Host is up (0.0022s latency).
MAC Address: B0:B2:8F:3E:59:
Nmap scan report for 192.16
Host is up (0.32s latency).
MAC Address: 60:01:94:CC:19
Nmap scan report for 192.16
Host is up (0.049s latency).
MAC Address: D8:7D:7F:09:21
Nmap scan report for 192.16
Host is up (0.068s latency).
Nmap scan report for 192.168.1.58
Host is up (0.32s latency).
MAC Address: 0E:97:4F:B5:E8:36 (Unknown)
Nmap scan report for 192.168.1.59
Host is up (0.00019s latency).
MAC Address: 40:A3:CC:85:B8:8A (Intel Corporate)
Nmap scan report for 192.168.1.60
Host is up (0.097s latency).
MAC Address: 60:01:94:CF:78:03 (Espressif)
Nmap scan report for 192.168.1.64
Host is up (0.21s latency).
MAC Address: A6:7F:81:12:FF:6F (Unknown)
```

פרטי הקורבן שלנו

פרויקט בקורס

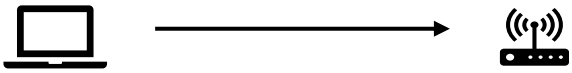
תקשורת מחשבים

4. על מנת לוודא כי אכן אלו כל פרטי הקורבן, נשתמש ב **ipcongif /all** שמחזירה את כל הפרטים.



כתובת MAC המזוהה גם בתור הכתובת הפיזית

בשלב זה המצב הוא:



Bob 192.168.1.59 **Alice** 192.168.1.1

5. בשלב זה, Eve נכנסת לתמונה, והיא "האיש שבאמצע".

בשלב זה נשתמש בכלי Ettercap- כלי לביצוע בדיקות אבטחה.
באמצעות כלי זה eth0 יהפוך להיות interface של Alice, כלומר של הנתב האלחוטי.
יעשה זאת באמצעות החלפת כתובת הMAC של הנתב בכתובתו שלו, כך למעשה כל החבילות שיצטרכו לעבור לשרת, יעברו ראשית אצלנו.

```
┌──(root💀kali)-[~]
└─# sudo ettercap -T -S -i eth0 -M arp:remote /192.168.1.1// /192.168.1.59//
```

בחלון זה נראה נוכל לאסוף מידע אודות הקורבן. ניתן לראות את הדוגמאות הבאות:

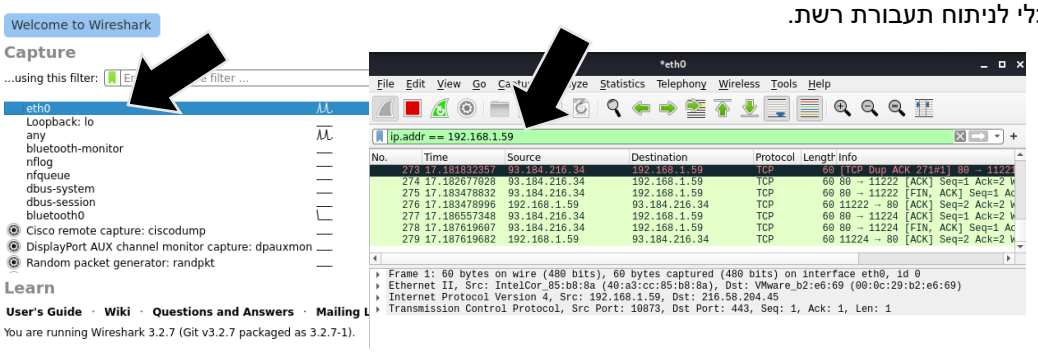
בשלב זה המצב הוא:

פרויקט בקורס

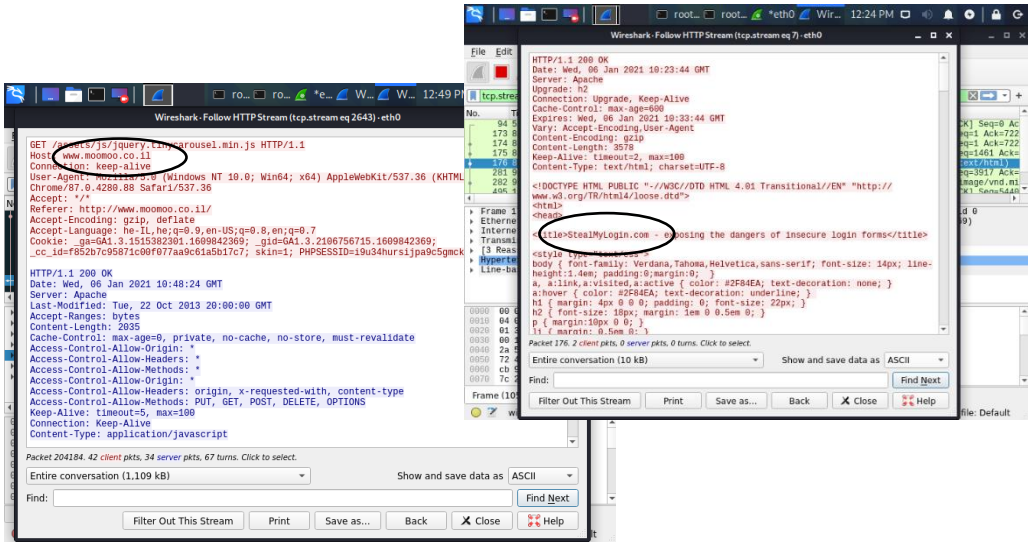
תקשורת מחשבים

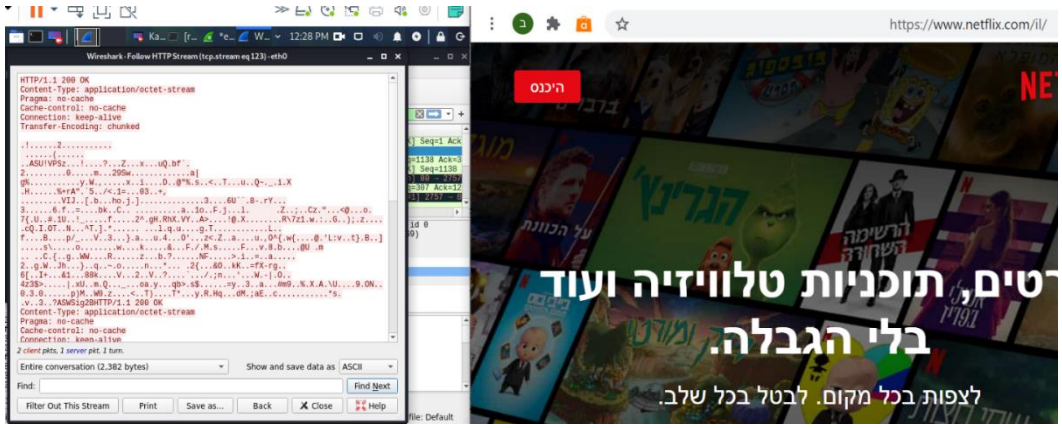
בשלבים הבאים נדלה מידע מהקורבן, נראה איזה מידע נוכל לדלות ואיזה לא.

6. בעזרת **wireshark** – כלי לניתוח תעבורת רשת.



דלינו את המידע הבא: בקשות http ותשובתם מהנתיב עבור אתרים הנמצאים בפרוטוקול http.





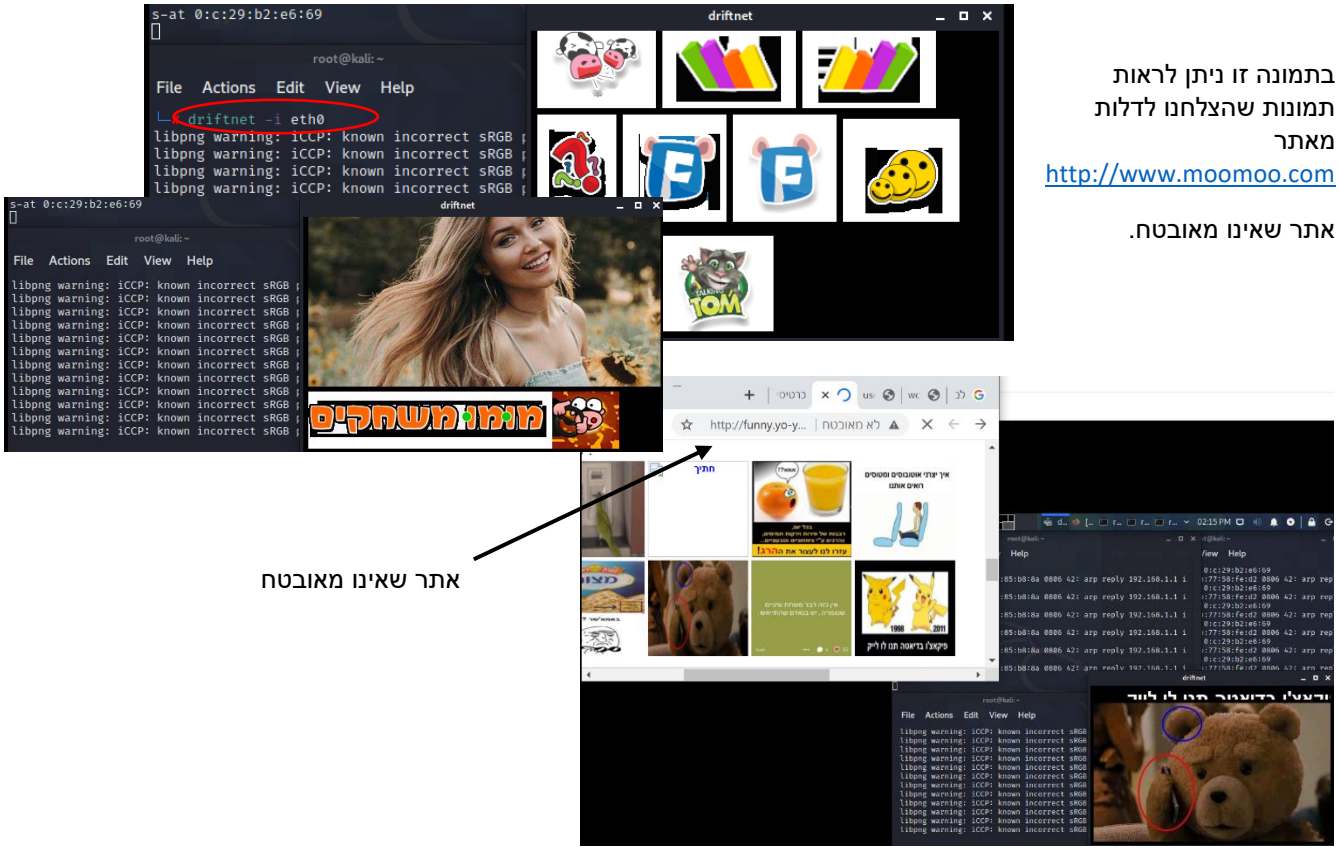
בקשות http עבור אתרים הנמצאים בפרוטוקול https. פרוטוקול מאובטח ולכן ניתן לראות כי הבקשה היא מוצפנת וקשה יותר לדלות מידע. (למידע נוסף עבור https ראה נספחים 2)

7. שימוש בכלי **driftnet** – כלי המאפשר לדלות תמונות.

בעזרת כתיבת הפקודה יפתח חלון נוסף ששם יופיעו התמונות אותן דלינו.

פרויקט בקורס

תקשורת מחשבים



בתמונה זו ניתן לראות תמונות שהצלחנו לדלות מאתר http://www.moomoo.com אתר שאינו מאובטח.

כלים לביצוע:

מערכת הפעלה מבוססת KALI – UNIX . הכוללת את הכלים הבאים:namp,Ettercap,wireshark,arpspoof .
דפדפן לשליחת בקשות URL ממכשיר הקורבן.
נתב אלחוטי ברשת מקומית.
יחידת קצה שתשמש כקורבן לתקיפה המחוברת לרשת האלחוטית המקומית.

תוצאות:

במהלך הניסוי אכן הצלחנו להרעיל את טבלת הARP של הקורבן ובכך לדלות מידע ותמונות המעידות על אופי הגלישה של הקורבן ברשת, באתרים המבוססים על פרוטוקול הhttp.
יש לציין כי את פרוטוקול https לא הצלחנו לפענח ולדלות מידע עבור אותו קורבן, לא צלחנו בדליית תמונות אך כן זיהינו את השרתים אליו פנה הקורבן.(ראה נספחים 2.2)

צפינו כי דליית המידע, התמונות וקריאת הבקשות יתבצעו באופן מהיר, אך בפועל נתקלנו בהמון קשיים שנבעו מהגורמים הבאים:
- רוב האתרים כיום מבוססים פרוטוקול https לעומת השנים הקודמות בהן הרוב היו מבוססים http, בעקבות כך לא צלחנו בדליית התמונות והמידע מהאתרים שרצינו והיינו צריכים לחפש אתרים מבוססי פרוטוקול http בלבד.
-בפנייה לאתרים המבוססים http נתקלנו בהגנה מצד מערכת ההפעלה ששמרה על פרטיותנו ורצתה למנוע מהמשתמש לחשוף את המידע.
- בעת ביצוע מתקפת ה"איש שבאמצע" נתקלנו בירידת מהירות הגלישה, בקשות http סורבו ו/או אושרו בזמן ארוך מהצפוי. (ראה נספחים 4)

לסיכום:

נראה כי בשנים האחרונות התקדמות הטכנולוגיה השפיעה על אבטחת המידע, מה שגרם למתקפת "האיש שבאמצע" להיות מסורבלת וקשה יותר מעבר לציפיות שהיו לנו בתחילת הפרויקט.
אנו בטוחים כי אם היינו מבצעים את אותו הניסוי לפני שנים ספורות בלבד היינו מקבלים תוצאות שונות.
ניתן לאפיין את אופיו של הקורבן על ידי גרפים וטבלאות שונים אותם נוכל להסיק מהכלי wireshark. (ראה נספחים 5)
ולבסוף, למדנו כי תעבורת הרשת הינה נושא רגיש.

פרויקט בקורס

תקשורת מחשבים

רשימת ספרות:

https://www.veracode.com/security/man-middle-attack

https://security.stackexchange.com/questions/8145/does-https-prevent-man-in-the-middle-attacks-by-proxy-server

https://www.speedtest.net/

https://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-simple-man-middle-attack-0147291/

https://he.wikipedia.org/wiki/%D7%94%D7%AA%D7%A7%D7%A4%D7%AA_%D7%90%D7%93%D7%9D_%D7%91%D7%AA%D7%95%D7%95%D7%9A

https://www.youtube.com/watch?v=uLo_kI1gcBc

נספחים:

1. השתמשנו בכלי נוסף כדי לדלות מידע מהקורבן. **ARPSPOOF** – כלי המאפשר שליחת הודעות arp שקריות שמרעילות את הקשר בין הנתב לבין הקורבן. נרעיל את שני הצדדים:

```
┌──(root💀 kali)-[~]
└─# arpspoof -i eth0 -t 192.168.1.1 192.168.1.59
```

```
┌──(root💀 kali)-[~]
└─# arpspoof -i eth0 -t 192.168.1.59 192.168.1.1
```

```
┌──(root💀 kali)-[~]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root💀 kali)-[~]
└─# cat /proc/sys/net/ipv4/ip_forward
1
```

אפשור המעבר שגורם "לאיש באמצע"

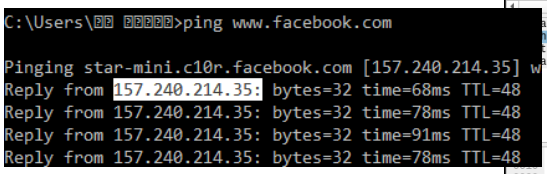
2. איך HTTPS עובד? פרוטוקול HTTPS מבוסס הצפנת מפתח ציבורי ופרטי, שזה אומר שהמפתח הציבורי משמש להצפנה והמפתח הפרטי משמש לפענוח.
ברגע שהדפדפן שולח בקשת HTTPS לשרת, השרת משיב עם מסמך והדפדפן בודק את תקינות המסמך לפי שני פרמטרים : * פרטי הבעלים צריכים להתאים לשם השרת אותו ביקש המשתמש ("זיהוי השרת").
* וידוא שלמות ההודעה, המסמך חייב להיות חתום בחתימה דיגיטלית על ידי השרת.
במידה ואחד מפרמטרים אלו אינו תקין, המשתמש מקבל דיווח על אודות הבעיה.
אחרי אישור תקינות המסמך, הדפדפן מחלץ את המפתח הציבורי ומשתמש בו על מנת להצפין מידע לפני השליחה לשרת, והשרת מסוגל לפענח את המידע כיוון שיש לו את המפתח הפרטי התואם.

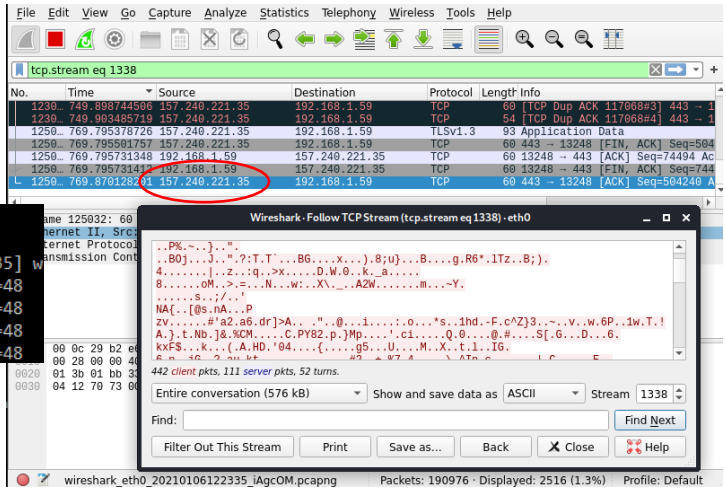
פרויקט בקורס

תקשורת מחשבים

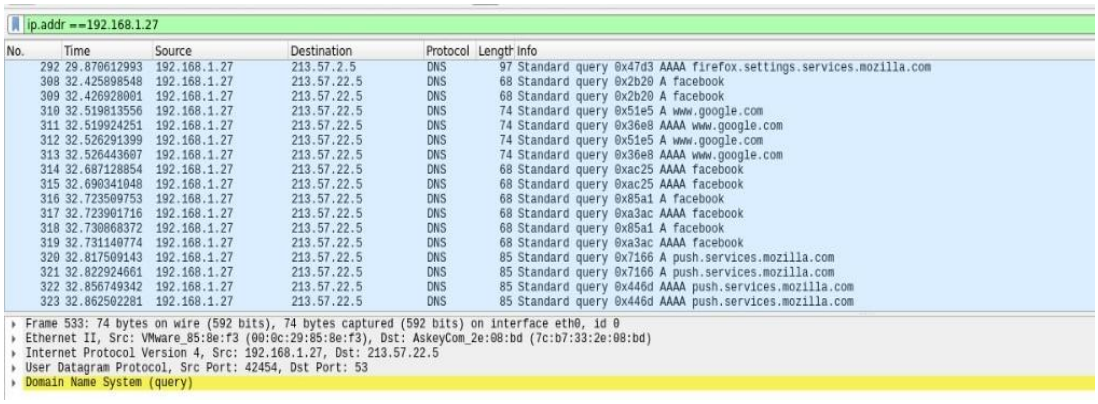
2.1 איך HTTPS מונע את התקפת "האיש שבאמצע"? האיש שבאמצע יוכל לחדור בין שני המשתמשים (במקרה שלנו, הנתב והקורבן) אך הוא לא יצליח לפענח את המידע המוצפן כיוון שאין ברשותו את המפתחות הרלוונטיים.

כפי שניתן לראות בתיעוד הבא, את כתובת הip של שרת facebook הצלחנו לאתר בכלי wireshark אך ההודעה אותה שלח השרת לקורבן לא הצלחנו לפענח.

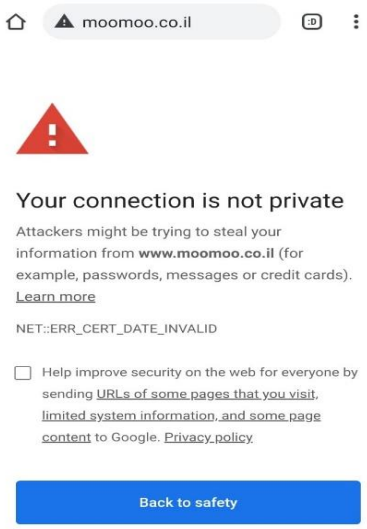




2.2 ניתוח אופיו של הקורבן לפי גלישתו ברשת.



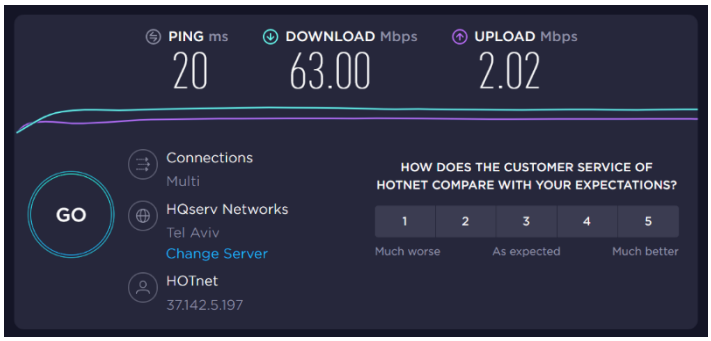
3. הגנת מערכת ההפעלה מהתקפת "האיש שבאמצע".



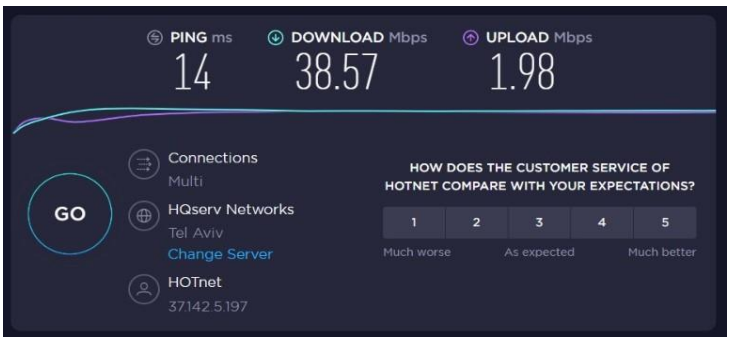
פרויקט בקורס

תקשורת מחשבים

4. מהירות הגלישה לפני המתקפה



מהירות הגלישה בעת המתקפה



*בוצע בעזרת speed-test מדפדפן במחשב הקורבן. (https://www.speedtest.net/)

5. גרף קבלת החבילות לאורך זמן :